AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (previously presented): A method of providing security for a computer connected to a data store via a server, the method comprising :

generating an authentication key based on a user name, a computer identifier, and a server user identifier;

receiving the authentication key, the user name, and the computer identifier;

parsing the authentication key to obtain a parsed user name, computer identifier, and server user identifier; and

validating the received user name and computer identifier using the parsed user name and computer identifier; and

when the received user name and the computer identifier match the parsed user name and the computer identifier, using the parsed server user identifier to acess the server,

wherein the user accesses the data store via the server using the generated authentication key, and wherein, when the server user identifier changes, a new authentication key is generated for the user and the user accesses the data store via the server using the new authentication key.

2. (original): The method of claim 1, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

3. (original): The method of claim 2, wherein a match indicates that the received user name and computer identifier are valid.

4. (original): The method of claim 1, further comprising, before parsing, decrypting the authentication key.

5. (previously presented): The method of claim 1, further comprising, if the received user name and computer identifier are valid, logging onto the server with the server user identifier and a server password.

6. (original): The method of claim 5, further comprising, parsing the authentication key to obtain the server user identifier and server password.

7. (original): The method of claim 6, wherein multiple users share one server user identifier and server password.

8. (canceled).

9. (previously presented): The method of claim 1, wherein the computer is connected to a client and the server and wherein the authentication key is generated with a client user name, a client computer identifier, the server user identifier, and a server password.

10. (previously presented): The method of claim 9, further comprising encrypting the authentication key.

11. (previously presented): The method of claim 9, further comprising forwarding the authentication key to a user.

12. (previously presented): The method of claim 1, wherein the computer is connected to a client and the server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

13. (previously presented): An apparatus for providing security, comprising:

a computer having a server connected thereto to access a data store;

one or more computer programs, performed by the computer, for generating an authentication key based on a user name and a computer identifier, said authentication key includes a server user name, receiving the authentication key, the user name, and the computer identifier, parsing the authentication key to obtain a parsed user name, computer identifier, and

server user name, and validating the received user name and computer identifier using the parsed user name and computer identifier,

wherein the user uses the parsed server user name to access the data store via the server, and

wherein, when the server user name changes, a new authentication key is generated for the user and the user accesses the data store via the server using the changed server user name obtained from parsing the new authentication key.

14. (original): The apparatus of claim 13, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

15. (original): The apparatus of claim 14, wherein a match indicates that the received user name and computer identifier are valid.

16. (original): The apparatus of claim 13, further comprising, before parsing, decrypting the authentication key.

17. (previously presented): The apparatus of claim 13, further comprising, if the received user name and computer identifier are valid, logging onto the server with the server user identifier and server password.

18. (original): The apparatus of claim 17, further comprising, parsing the authentication key to obtain the server user identifier and server password.

19. (original): The apparatus of claim 18, wherein multiple users share one server user identifier and server password.

20. (canceled).

21. (previously presented): The apparatus of claim 13, wherein the computer is connected to a client and the server and wherein the authentication key is generated with a client user name, a client computer identifier, the server user identifier, and a server password.

22. (previously presented): The apparatus of claim 21, further comprising encrypting the authentication key.

23. (previously presented): The apparatus of claim 21, further comprising forwarding the authentication key to a user.

24. (previously presented): The apparatus of claim 13, wherein the computer is connected to a client and the server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

25. (previously presented): An article of manufacture comprising a computer program carrier readable by a computer connected to a server and embodying one or more instructions executable by the computer to perform method steps for providing security to the server connected to a data store, the method comprising:

generating an authentication key that includes a server user identifier, based on a user name and a computer identifier;

receiving the authentication key, the user name, and the computer identifier;

parsing the authentication key to obtain a parsed user name, computer identifier, and server user name; and

validating the received user name and computer identifier using the parsed user name and computer identifier,

wherein the user uses the parsed server user name to access the data store via the server, and

wherein, when the server user name changes, a new authentication key is generated for the user and the user accesses the data store via the server using the changed server user name obtained from parsing the new authentication key.

26. (original): The article of manufacture of claim 25, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

27. (original): The article of manufacture of claim 26, wherein a match indicates that the received user name and computer identifier are valid.

28. (original): The article of manufacture of claim 25, further comprising, before parsing, decrypting the authentication key.

29. (previously presented): The article of manufacture of claim 25, further comprising, if the received user name and computer identifier are valid, logging onto the server connected to the computer with the server user identifier and server password.

30. (original): The article of manufacture of claim 29, further comprising, parsing the authentication key to obtain the server user identifier and server password.

31. (original): The article of manufacture of claim 30, wherein multiple users share one server user identifier and server password.

32. (canceled).

33. (previously presented): The article of manufacture of claim 25, wherein the computer is connected to a client and the server and wherein the authentication key is generated with a client user name, a client computer identifier, the server user identifier, and a server password.

34. (previously presented): The article of manufacture of claim 33, further comprising encrypting the authentication key.

35. (previously presented): The article of manufacture of claim 33, further comprising forwarding the authentication key to a user.

36. (previously presented): The article of manufacture of claim 25, wherein the computer is connected to a client and the server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

37. (previously presented): The method of claim 9, wherein the generated authentication key for access to the server is sent to a user, and further comprises a server password, and wherein when the server password changes, a unique new authentication key based on the server user identifier and the server password is sent to the user.

38. (previously presented): The method of claim 37, wherein when the client transmits the generated authentication key, the user name and the computer identifier, to the server, the authentication key is interecepted and validated by the computer.

39. (previously presented): The method of claim 38, wherein when the computer determines that the received user name and the computer identifier match the parsed user name and the computer identifier, the computer parses the authentication key to obtain the server user identifier and the server password.

40. (previously presented): The method of claim 39, wherein the parsed server user identifier and the parsed server password is transmitted to the server, connecting the client computer to the server.

41. (previously presented): The method of claim 9, wherein the authentication key comprises the computer identifier split into portions and the portions being interposed between the user name, the server user identifier and the server password prior to encryption.

42. (previously presented): The method according to claim 9, wherein the computer identifier is an IP address.

43. (currently amended): A method of ~~A method of~~ facilitating security maintance in a secure access to a data store via a server, the method comprising:

each time ~~the~~ a user logs onto a ~~clien~~ client workstation with a computer identifier, generating an authentication key based on a server identifier, a server password, a user name, and the computer identifier;

receiving the authentication key, the user name, and the computer identifier;

parsing the authentication key to obtain a parsed user name, computer identifier, server identifier, and server password; and

validating the received user name and computer identifier using the parsed user name and computer identifier; and

accessing the data store via the server using the parsed server identifier and the parsed server password,

wherein when the administrator changes the server password, a new authentication key is generated and transmitted to the user for access to the data store.

44. (previously presented): The method of claim 1, wherein the authentication key comprises a plurality of fields, and wherein a first field type stores a portion of the computer identifier, a second field type stores at least one the server user identifier, a server password, the user name, and a third field type comprises a separator.

45. (previously presented): The method of claim 1, wherein the user accesses the data store via the server using a unique authentication key generated using the user name, the

computer identifier, the server user identifier, and a server password that corresponds to the server user identifier, and wherein, when the administrator changes the server password, a new authentication key is generated for the user and the user accesses the data store via the server using the new authentication key.

46. (previously presented): The method of claim 1, wherein a plurality of authentication keys for different users are generated using the server user identifier, and wherein, when the server user identifier changes, a plurality of new authentication keys are generated for the different users and each of the generated plurality of new authentication keys is transmitted to respective user.